Auditing the LAN with Network Discovery

Introduction

This application note is one in a series of papers about troubleshooting local area networks (LAN) from JDSU Communications Test and Measurement. Auditing the LAN can be achieved by conducting a Network Discovery. The Network Discovery process "learns" which devices are attached to the network and provides valuable information such as Internet Protocol (IP) addresses, Media Access Controller (MAC) addresses, virtual LAN (VLAN) configuration, and device configuration information.

Typical uses for Network Discovery include:

- identifying the types of devices that are attached to the network (routers, switches, workstations, hosts, printers, and others)
- assisting with on-site troubleshooting (for example, data center or remote office) by verifying that a new server or host is actually online, without the need for an enterprise Network Operations Center (NOC) system management tool
- verifying the devices that are attached to the network are supposed to be attached to the network (for example, detect wireless access ports or personal computers [PCs])
- detecting device anomalies such as high switch port collisions and Frame Check Sequence (FCS)—on site and without the need for an enterprise NOC system management tool
- identifying specific switch and router interfaces with high utilization before utilizing active taps or configuring mirror ports.

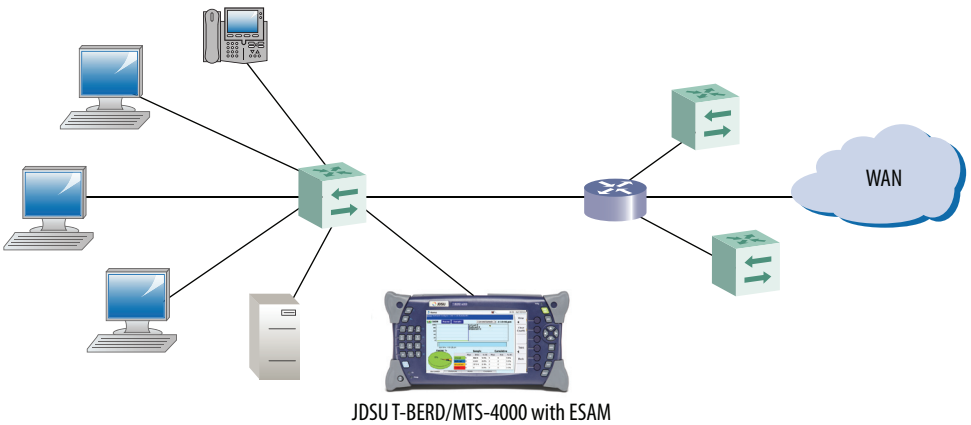


Figure 1: JDSU T-BERD®/MTS-4000 (with ESAM) connected to a normal switch port

Network Discovery does not require the special port monitoring access mode. As Figure 1 shows, the JDSU Enterprise Services Application Module (ESAM) can connect to standard office wall jacks or switch ports to conduct Network Discovery tests.

Network Discovery relies on a sophisticated combination of passive and active techniques that allows the ESAM to accurately detect and identify hosts on and off of the local subnet.

Network Discovery Workflow

This application note demonstrates use cases for LAN network discovery and provides examples using the JDSU ESAM for the T-BERD/MTS-4000. As Section 1 references, Network Discovery does not require special monitoring access and the ESAM connects just as any other host to normal office LAN ports, switch ports, and others.

It is common to enter a data center or other central networking location to gain basic insight into the network, such as which subnet is present and are the expected switches and routers present. Figure 2 illustrates a basic network diagram of a small and medium business (SMB) office location.

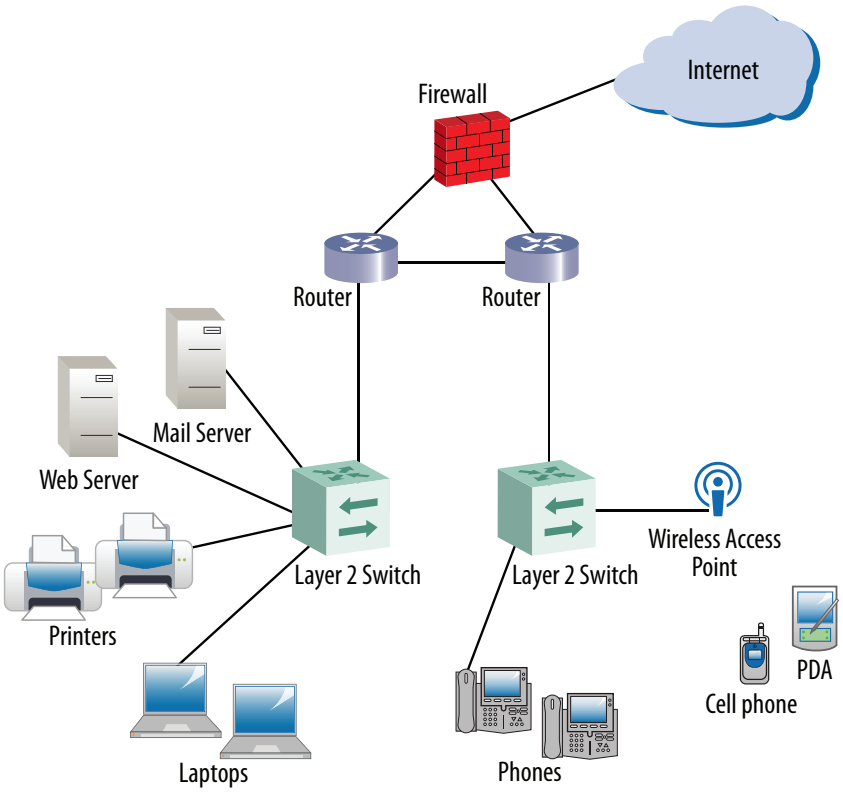


Figure 2: Typical SMB Office Network

For a Network Discovery audit, technicians can connect the JDSU ESAM to a spare office LAN wall jack or spare interface on one of the switches. Figure 3 shows the summary results screen received after the ESAM conducts network discovery.

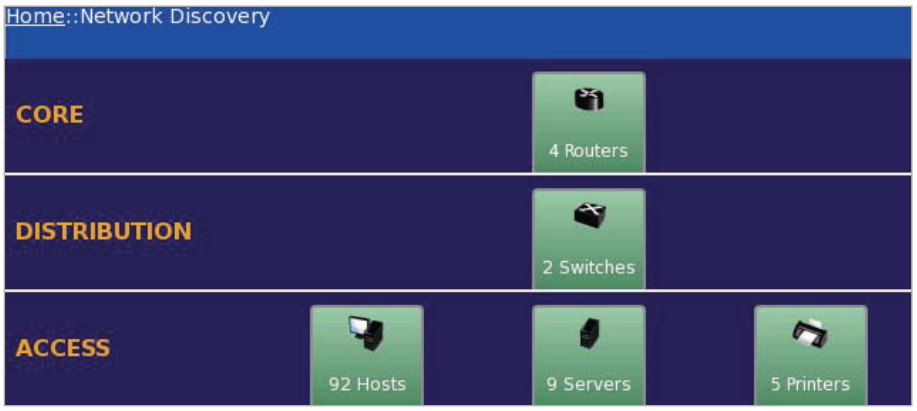


Figure 3: Network Discovery Result

The devices are logically layered based on the Cisco network reference model: Access, Distribution, and Core. Although this reference model is Cisco-based, the IT community widely uses and understands it.

The following subsections describe a recommended workflow after obtaining the network discovery results but are not intended to imply that this workflow is static. Depending upon the diagnostic question that must be answered, users will likely navigate directly to a problem device or host.

Basic Interpretation of Network Discovery Results

The first question to answer after a network discovery might be: are these the devices that should be on the network? Based upon the discovery results shown in Figure 3, these were the devices detected:

- 9 servers
- 92 hosts (or workstations)
- 5 printers
- 2 switches
- 4 routers.

Scanning the workstations, it is easy to determine the overall summary of connected hosts by clicking on the Hosts icon as shown in Figure 4. This table summarizes Workstation IP addresses, Windows host names, and other information.

Home::Network Discovery::Hosts

SNMP	DNS Name	IP Address	MAC Address	NetBIOS Name
Show	germfd2500-3.ger.am.acterna.net	10.10.46.32	00:00:74:E0:69:42	RNPE06942
Show	germfd3000-6.ds.jdsu.net	10.10.46.30	00:00:74:E1:3D:2D	RNPE13D2D
Show	germfd3000-4.ds.jdsu.net	10.10.46.16	00:00:74:E0:75:56	RNPE07556
Show	ger2500-2.ds.jdsu.net	10.10.46.13	00:00:74:DD:E0:C8	RNPDDE0C8
N/A	gerlx-c3s14j1.ds.jdsu.net	10.10.46.96	00:21:70:D1:CE:C7	GERLX-C3S14J1
N/A	gerdx-lkbwhyv.ds.jdsu.net	10.10.46.43	00:1E:37:2C:12:F6	GERDX-LKBWHYV

Figure 4: Drilling into Hosts from the Discovery Summary Screen

As Section 1 mentioned, the network discovery process is sometimes used to determine if devices are present on the network that should not be. Based on this case, the network manager realizes that the number of routers should have equaled 3 and needs to investigate the presence of the fourth router.

Clicking the Router icon on the ESAM user interface provides a list of Routers along with their source MAC addresses as Figure 5 shows.

Home::Network Discovery::Routers

SNMP	IP Address	MAC Address
NO	10.10.46.3	00:22:BE:EA:FC:00
NO	10.10.46.1	00:00:0C:07:AC:01
NO	10.10.46.2	00:22:BE:72:5C:00
NO	192.168.15.1	00:1D:7E:D6:66:E2

Figure 5: Drilling into Routers from the Discovery Summary Screen

The detailed Routers table shows three Cisco devices (expected) and an unexpected Cisco-Linksys® device. The unauthorized Linksys device is a wireless access point that is installed on an enterprise network, which is a fairly common occurrence.

All network devices have a 6-byte Ethernet MAC address in the form of 00:22:BE:EA:FC:00.The first three bytes are referred to as the Organization Unique Identifier (OUI) that identifies the company that manufactured the network device.

In this case, 00:22:BEs and the 00:00:0C OUIs belong to Cisco Systems, but the 00:1D:7E OUI belongs to Cisco-Linksys, which is the wireless company within Cisco.The IEEE maintains a list of OUIs and their associated companies.The link to look up OUIs is http://standards.ieee.org/regauth/oui/index.shtml.

Detailed Interpretation of Specific Devices

Beyond the basic network device survey, it is important to know which links are consuming excessive bandwidth or which links exhibit excessive errors, such as FCS errors, collisions, and other errors. Obtaining this detailed device information requires enabling Simple Network Management Protocol (SNMP) access on the device and allowing the ESAM access to the SNMP community string (a text string that acts as a password).

Figure 6 shows the examination of an SNMP enabled edge switch.

SNMP	MAC Address	VLAN	Alarm
NO	00:08:21:38:6D:22	VLAN	Alarm
YES	00:03:6B:C1:97:80	VLAN	Alarm

Interfaces

If	Description	Speed	Op Status
15	FastEthernet0/3	100M	up
16	FastEthernet0/4	100M	down
17	FastEthernet0/5	100M	up
18	FastEthernet0/5	100M	up
19	FastEthernet0/7	100M	up
20	FastEthernet0/8	100M	down
22	FastEthernet0/9	100M	up
23	FastEthernet0/10	100M	down
24	FastEthernet0/11	100M	up
25	FastEthernet0/12	100M	up
31	GigabitEthernet0/1	1G	down

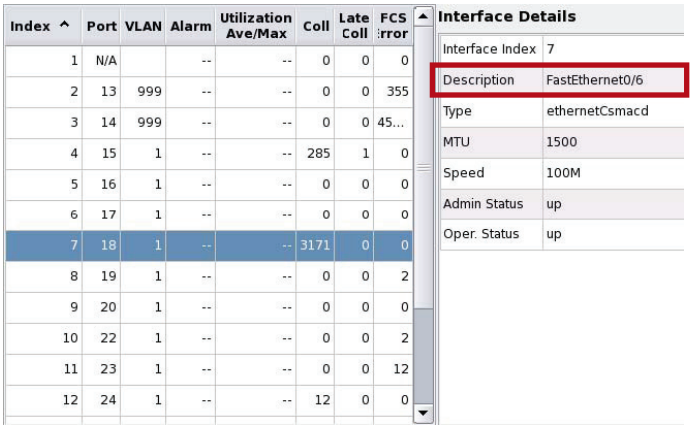
Figure 6: Interface Summary of an SNMP Enabled Switch

SNMP is widely used to manage LAN networks. Devices that support SNMP store various configuration and performance information in a Managed Information Base (MIB) that can be queried via an SNMP client or management console. The SNMP client can query an SNMP agent (device) to obtain MIB information such as vendor name, software version, hardware specifications, and performance statistics such as CPU utilization, network port errors, and utilization to name a few.

Access to the SNMP functionality is controlled via an SNMP community string that is used to authenticate messages sent between the SNMP manager and the SNMP agent. Most IT administrators have access to the SNMP community "read" string, which permits SNMP management tools to poll the SNMP agents and retrieve the SNMP MIB information.

The JDSU ESAM supports SNMP version v1, v2c, or v3.

The interface summary clearly shows the number of interfaces for the switch and the operational status as well "up/down". For even more detailed information, drill into a specific port as the Interface Details view in Figure 7.



Index	Port	VLAN	Alarm	Utilization Ave/Max	Coll	Late Coll	FCS rror
1	N/A		--	--	0	0	0
2	13	999	--	--	0	0	355
3	14	999	--	--	0	0	45...
4	15	1	--	--	285	1	0
5	16	1	--	--	0	0	0
6	17	1	--	--	0	0	0
7	18	1	--	--	3171	0	0
8	19	1	--	--	0	0	2
9	20	1	--	--	0	0	0
10	22	1	--	--	0	0	2
11	23	1	--	--	0	0	12
12	24	1	--	--	12	0	0

Interface Details

Interface Index	7
Description	FastEthernet0/6
Type	ethernetCsmacd
MTU	1500
Speed	100M
Admin Status	up
Oper. Status	up

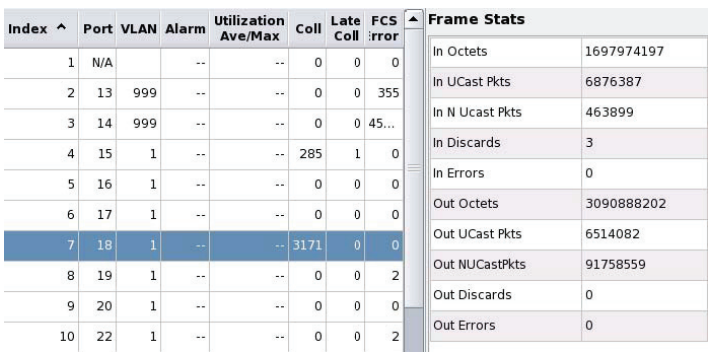
Figure 7: Interface Details View of an SNMP Enabled Switch

In Figure 7, the reported SNMP port 18 is drilled into which corresponds to switch port "FastEthernet 0/6". This detailed information of switch port FastEthernet 0/6 provides the following interface information:

- VLAN ID = 1
- MTU = 1500
- Collision count = 3171
- FCS Errors = 0

From the information provided, the network troubleshooter may discover that the port is associated with the incorrect VLAN, the maximum transmission unit (MTU) size is not as expected, or may want to investigate the cause for the high collision count on this port.

Figure 8 shows the Frame Stats view that provides more detailed interface usage statistics. It shows the total number of ingress and egress octets as well as discards and errored octets, which also provides valuable insight into possible congestion (discards) and FCS-error frames.



Index	Port	VLAN	Alarm	Utilization Ave/Max	Coll	Late Coll	FCS rror
1	N/A		--	--	0	0	0
2	13	999	--	--	0	0	355
3	14	999	--	--	0	0	45...
4	15	1	--	--	285	1	0
5	16	1	--	--	0	0	0
6	17	1	--	--	0	0	0
7	18	1	--	--	3171	0	0
8	19	1	--	--	0	0	2
9	20	1	--	--	0	0	0
10	22	1	--	--	0	0	2

Frame Stats

In Octets	1697974197
In UCast Pkts	6876387
In N Ucast Pkts	463899
In Discards	3
In Errors	0
Out Octets	3090888202
Out UCast Pkts	6514082
Out NUCastPkts	91758559
Out Discards	0
Out Errors	0

Figure 8: Frame Stats View of an SNMP Enabled Switch

Conclusion

Gaining visibility into the LAN is an important first step in many LAN troubleshooting exercises. It is important to verify the presence of devices attached to the networks as well as unauthorized devices that should not be there. Network discovery accomplishes this by quickly establishing the baseline—what is attached to the network—and then determining what the attached devices are doing on the network.

The JDSU ESAM for the T-BERD/MTS-4000 provides a workflow-based interface that "walks" users through the best practices approach toward solving a multitude of network problems. Figure 9 illustrates the JDSU ESAM interface and Figure 10 shows the workflow-based user interface.

Figure 9: JDSU T-BERD/MTS-4000 platform with the ESAM

Figure 10: Workflow Based User Interface of the ESAM

The JDSU ESAM for the T-BERD/MTS-4000 provides comprehensive LAN testing capability with these features:

- Layer 1-7 protocol capture and expert analysis
- network connectivity
- network discovery
- a full range of physical media tests
- a workflow-based user interface
- a modular platform with many options:
  - VoIP phone emulation
  - optical power meter/visual fault locator
  - fiber inspection probe with automated pass/fail
  - Wireless fidelity (WiFi) testing
  - OTDR modules

Through its workflow-based intuitive user interface, the ESAM provides physical media tests including speed-certification of electrical Ethernet cabling, network connectivity tests, discovery, wirespeed deep-packet statistics, and wirespeed protocol capture and expert analysis using unique, in-depth JDSU J-Mentor capabilities. In addition, the ESAM is part of the modular JDSU T-BERD/MTS-4000 platform allowing additional options that include voice over IP (VoIP) emulation, WiFi testing, IP video testing, optical power meters (OPMs), visual fault locators (VFLs), digital fiber inspection probes, and Optical time domain reflectometers (OTDRs). Test connectivity can be obtained either electrically via a 10/100/1000 RJ45 Ethernet jack or via an SFP for optical Ethernet.

Test & Measurement Regional Sales

NORTH AMERICA
TEL: 1 866 228 3762
FAX: +1 301 353 9216

LATIN AMERICA
TEL: +1 954 688 5660
FAX: +1 954 345 4668

ASIA PACIFIC
TEL: +852 2892 0990
FAX: +852 2892 0770

EMEA
TEL: +49 7121 86 2222
FAX: +49 7121 86 1222

WEBSITE: www.jdsu.com/esam